UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/508,840	03/08/2005	Christophe Genevois	740612-187	9829

41972 7590 03/17/2008

LAW OFFICES OF STUART J. FRIEDMAN
28930 RIDGE ROAD
MT. AIRY, MD 21771

EXAMINER	
PHAM, LUU T	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/508,840	GENEVOIS, CHRISTOPHE	
	Examiner	Art Unit	
	LUU PHAM	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/14/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the application 10/508,840 filed on 09/21/2004.

2. Claims 1-39 have been examined and are pending.

Claim Objections

3. **Claims 6, 14, 21, 23, 25, and 27 are objected to under 37 CFR 1.75(c)** because of the following informalities:

- **Regarding claim 6**, the acronyms "DVB", "EMM", "CAS" and "SIM" are used without spelling out in full at their first occurrences in the claim. Appropriate corrections are required.

- **Regarding claim 14**, the acronym "GSM" is used without spelling out in full at its first occurrence in the claim. Appropriate correction is required.

- **Regarding claim 23**, the acronyms "PCMCIA" and "SCR" are used without spelling out in full at their first occurrences in the claim. Appropriate corrections are required.

- **Regarding claim 21**, the claim recites "*the system of any of claims 1 to 19 claim 3.*" There is insufficient antecedent basis for this limitation in the claim. For the purpose of applying art, the examiner interprets "*the system of any of claims 1 to 19 claim 3,*" to mean "*the system of claim 3.*"

- **Regarding claim 25**, the acronym "DCT" is used without spelling out in full at its first occurrences in the claim. Appropriate correction is required.

- **Regarding claim 27**, the claim recites "*the system of any of claims 1 to 24 claim 3.*" There is insufficient antecedent basis for this limitation in the claim. For the purpose of applying art, the examiner interprets "*the system of any of claims 1 to 24 claim 3,*" to mean "*the system of claim 3.*"

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 1-33 and 36-39 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- **Regarding claims 1 and 2**, the claims recite "*A conditional access system.*" However, there is not any element in the system.

- **Regarding claims 3-33 and 38-39**, claims 3-33 and 38-39 are dependent on claim 1 or 2, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

- **Regarding claim 36**, the claim recites *"A method of producing."* However, the steps of the method are not positively recited.

- **Regarding claims 37**, claim 37 is dependent on claim 36, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

- **Regarding claims 33 and 39**, the claims recite "*capable of detecting **at least some** of the following encryption levels*" (emphasis added). This is vague in reference to how many items would be necessary to be considered as 'some'. For the purpose of applying art, the examiner interprets the term "*capable of detecting **at least some** of the following encryption levels*" to mean "*capable of detecting **at least one** of the following encryption levels.*" (emphasis added). Appropriated corrections are required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. **Claims 1-3, 11-13, 15, 20-22, and 24-29 are rejected under 35 U.S.C. 101** because the claims may be directed to non-statutory subject matter.

- **Regarding claims 1 and 2**, the claims recite "*A conditional access system;*" however, the claim is directed to software implementation, and they do not recite any elements or hardware. Therefore, the claimed subject matter does not belong to any of the four statutory categories set forth above.

- **Regarding claims 3, 11-13, 15, 20-22, and 24-29**, claims 3, 11-13, 15, 20-22, and 24-29 are also rejected as nonstatutory under 35 U.S.C. 101 as they do not recite any elements or hardware.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. **Claim 1-3, 7-8, 11-13, 15, 17, 19-22, 24-35, and 38-39 are rejected under 35 U.S.C. 102(e)** as being anticipated by Candelore, U.S. Patent Application No. 2003/0081776, filed on January 02, 2002.

- **Regarding claim 1**, Candelore discloses a conditional access system *(par. 0006; Conditional access (CA) systems are used to control availability of programming in content delivery systems such as cable systems)* wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets *(pars. 0010, 0046, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, wherein a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream *(pars. 0064 and 0089; Figs. 4 and 7; packets are selected at 250 and 350)*, removing and encrypting the particular data packets with an event encryption key *(pars. 0064 and 0089; Figs. 4 and 7; selected packets are passed for encryption to packet encryption process A at step 258 and packet encryption process B at step 262)*, and inserting the encrypted data packets into the

remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport system *(pars. 0054-0055, 0064-0068, and 0089; Figs. 3-4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; packet is encrypted as a part of the encryption time slice; the EA and EB packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same).*

- **Regarding claim 2**, Candelore discloses a conditional access system *(par. 0006; Conditional access (CA) systems are used to control availability of programming in content delivery systems such as cable systems)* wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets *(pars. 0010, 0046, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, wherein a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream *(pars. 0064 and 0089; Figs. 4 and 7; packets are selected at 250 and 350)*, removing and encrypting the particular data packets with an event encryption key *(pars. 0064 and 0089; Figs. 4 and 7; selected packets are passed for encryption to packet encryption process A at step 258 and packet encryption process B at step 262)*, and inserting the encrypted data packets into the remaining base transport stream at insertion positions corresponding to the original positions of the particular data packets in the base transport system *(pars. 0064 and 0089; Figs. 4 and 7; the encrypted selected packets are passed on to 254 for insertion into the*

output stream; the EA and EB packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same).

- **Regarding claim 3,** Candelore discloses the system of claim 1 or claim 2, wherein an event decryption key is provided to an authorized receiver provided with the conditional access system *(par. 0046; authorized set-top boxes receive Entitlement Control Messages (ECM) that are used to get access criteria and descrambling key)*, the selectively encrypted transport stream is transmitted to the receiver *(pars. 0043 and 0065; Figs. 3-8; after distribution through the cable system 32, the video, system information, program specific information, Audio A and Audio B are all delivered to set-top boxes 36 and 136)*, the conditional access system detects encrypted data packets, removes the encrypted data packets from the received transport stream, decrypts the encrypted data packets with the event decryption key *(pars. 0065-0069 and 0090; Figs. 5 and 8; when a packet is received at 272, it is inspected to see if it has the primary and secondary PID of interest (step 272 and 274); if the packet has the primary PID of interest, the packet is examined at 284 to determine if the packet is encrypted; if the packet has the secondary PID at 274, the packet is then decrypted at 296 and sent to the packet decoder at 288)*, and inserts the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the base transport stream *(pars. 0063-0067 and 0090; Figs. 5 and 8; packets encrypted under CA system B with the secondary PID are decrypted by CA system B 240 and inserted into the clear data stream for decoding and display on television set 244).*

- **Regarding claim 7**, Candelore discloses the system of claim 3, wherein the conditional access system has a buffer memory to store clear data packets while an encrypted data packet is decrypted *(pars. 0144-0145; Figs. 17-18; buffers 1006, 1014, 1024, and 1032)*.

- **Regarding claim 8**, Candelore discloses the system of claim 3, wherein said encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions *(pars. 0064 and 0089; Figs. 4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; the EA and EB packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same)*.

- **Regarding claim 11**, Candelore discloses the system of claim 3, wherein the decryption key is transmitted to a receiver with the selectively encrypted data stream *(par. 0010; additional packets are also included to provide decryption keys and other overhead information)*.

- **Regarding claim 12**, Candelore discloses the system of claim 11, wherein the event decryption key is frequently changed *(pars. 0040 and 0082; packets encrypted with Motorola's proprietary encryption can use fast changing encryption keys using the embedded security ASIC)*.

- **Regarding claim 13**, Candelore discloses the system of claim 3, wherein the event decryption key is a fixed key distributed on a pay-per-event basis *(par. 0046; descrambling keys are only distributed to authorized set-top boxes)*.

- **Regarding claim 15**, Candelore discloses the system of claim 3, wherein the event decryption key is provided encrypted with a user encryption key and a corresponding user decryption key is also provided to an authorized user *(par. 0046; authorized set-top boxes receive Entitlement Control message that are used to get access criteria and descrambling keys)*.

- **Regarding claim 17**, Candelore discloses the system of claim 3, comprising a head-end encoder for producing the selectively encrypted data stream, the head-end encoder including a Common Interface CI for a PC card module that has encryption circuitry thereon *(pars. 0118, 0121, and 0144)*.

- **Regarding claim 19**, Candelore discloses the system of claim 3, comprising a head-end encoder for producing the selectively encrypted data stream *(pars. 0046, 0055, 0073, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, the head-end encoder including an encoder CI module with a CI&TS (Common Interface and Transport Stream) interface to a professional Set-Top-Box STB *(Figs. 2-10; cable system head-end 122 transmits data stream to set-top boxes 36 and 136)*.

- **Regarding claim 20**, Candelore discloses the system of claim 3, wherein the base data stream is a clear data stream *(par. 0039; substantial portions of content is in clear while encrypting is only a small portions of content)*.

- **Regarding claim 21**, Candelore discloses the system of any of claims 1 to 19 claim 3, wherein the base data stream is a DVB-scrambled data stream *(pars. 0005-0006 and 0043; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44)*.

- **Regarding claim 22**, Candelore discloses the system of claim 3, wherein all data packets other than the selectively encrypted data packets are DVB-scrambled *(pars. 0045 and 0051; the SI may be scrambled to make it more difficult for a non-authorized set-top boxes)*.

- **Regarding claim 24**, Candelore discloses the system of claim 3, wherein said particular data packets are of a nature such that their contents are propagated to successive data packets *(pars. 0010, 0037, and 0038; packet streams for each component of all programs carried within a channel are aggregated into one composite stream)*.

- **Regarding claim 25**, Candelore discloses the system of claim 3, wherein said particular data packets are data packets containing sign bits of DCT coefficients in an MPEG stream *(pars. 0048, 0077, 0079, and 0084-0087; VCT access control bit is set)*.

- **Regarding claim 26**, Candelore discloses the system of claim 3, wherein every n^{th} data packet of the transport stream is encrypted, n being a fixed number *(pars. 0056 and*

0072-0075; tables 1-2; packets having any of the above four PIDs are again encrypted followed by the next eight time periods being sent in the clear).

- **Regarding claim 27,** Candelore discloses the system of any of claims 1 to 24 claim 3, wherein every n^{th} data packet of the transport stream is encrypted, n being a variable number *(pars. 0072-0075; random value m and n are known as variable numbers).*

- **Regarding claim 28,** Candelore discloses the system of claim 27, wherein the variable number n is randomly variable *(pars. 0072-0075; pseudo-random and semi-random values for m and n may be used for selection of packets to encrypt).*

- **Regarding claim 29,** Candelore discloses the system of claim 27, wherein the variable number n is variable as a function of data packet contents *(pars. 0072-0075; pseudo-random and semi-random values for m and n may be used for selection of packets to encrypt).*

- **Regarding claim 30,** Candelore discloses the system of claim 3, wherein the conditional access system is embedded in a user Set-Top-Box (STB) *(pars. 0006 and 0063-0065; Figs. 2-6; set-top box 36 includes conditional access system 40).*

- **Regarding claim 31,** Candelore discloses the system of claim 3, wherein said conditional access system includes a PC card with a Common Interface CI for connection to a user Set-Top-Box (STB) *(par. 0006; CA systems come as matched sets – one part is integrated into the cable system head-end and encrypts premium content, the other part provides decryption and is built into the STB).*

- **Regarding claim 32**, Candelore discloses the system of claim 30, wherein said user Set-Top-Box (STB) is capable of detecting a current encryption level of the transport stream and to direct the transport stream, in accordance with the detected encryption level, to decryption circuitry associated with that encryption level *(pars. 0037, 0043, 0047-0048; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44; the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box).*

- **Regarding claim 33**, Candelore discloses the system of claim 30, wherein the user Set-Top-Box (STB) is capable of detecting at least some of the following encryption levels of the transport stream:

None

DVB only

DVB and selective encryption *(pars. 0037, 0043, 0047-0048; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44; the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box).*

Selective encryption only; and

the Set-Top-Box (STB) is capable of directing the transport stream to at least one of the following decryption means:

None

An embedded conditional access system in the Set-Top-Box (STB) able to cope with DVB only,

An embedded conditional access system in the Set-Top-Box (STB) able to cope with selective encryption only,

An embedded conditional access system in the Set-Top-Box (STB) able to cope with DVB and with selective encryption *(pars. 0043, 0047-0048; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44)*,

A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB only,

A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-box (STB) able to cope with selective encryption only,

A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB and with selective encryption, A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB only,

A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-box (STB) able to cope with selective encryption only,

A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB and with selective encryption, A Smart Card (SC) in a Smart Card Reader (SCR).

- **Regarding claim 34**, Candelore discloses a method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitized multimedia data in successive data packets *(pars. 0010, 0046, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, wherein a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream *(pars. 0064 and 0089; Figs. 4 and 7; packets are selected for encryption at 250 and 350)*, removing and encrypting the particular data packets with an event encryption key *(pars. 0064 and 0089; Figs. 4 and 7; selected packets are passed for encryption to packet encryption process A at step 258 and packet encryption process B at step 262)*, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the clear transport stream *(pars. 0054-0055, 0064-0068, and 0089; Figs. 3-4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; packet is encrypted as a part of the encryption time slice; the EA and EB packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same)*.

- **Regarding claim 35**, Candelore discloses a method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitized multimedia data in successive data packets *(pars. 0010, 0046, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are*

selected and encrypted and transmitted to cable system 32), wherein a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream *(pars. 0064 and 0089; Figs. 4 and 7; packets are selected for encryption at 250 and 350)*, removing and encrypting the particular data packets with an event encryption key *(pars. 0064 and 0089; Figs. 4 and 7; selected packets are passed for encryption to packet encryption process A at step 258 and packet encryption process B at step 262)*, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream *(pars. 0064 and 0089; Figs. 4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; the EA and EB packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same)*.

- **Regarding claim 38,** Candelore discloses the system of claim 31, wherein said user Set-Top-Box (STB) is capable of detecting a current encryption level of the transport stream and to direct the transport stream, in accordance with the detected encryption level, to decryption circuitry associated with that encryption level *(pars. 0037, 0043, 0047-0048; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44; the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box)*.

- **Regarding claim 39**, Candelore discloses the system of claim 31, wherein the user Set-Top-Box (STB) is capable of detecting at least some of the following encryption levels of the transport stream:

None

DVB only

DVB and selective encryption *(pars. 0037, 0043, 0047-0048; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44; the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box).*

Selective encryption only; and

the Set-Top-Box (STB) is capable of directing the transport stream to at least one of the following decryption means:

None

An embedded conditional access system in the Set-Top-Box (STB) able to cope with DVB only,

An embedded conditional access system in the Set-Top-Box (STB) able to cope with selective encryption only,

An embedded conditional access system in the Set-Top-Box (STB) able to cope with DVB and with selective encryption *(pars. 0043, 0047-0048; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44)*,

A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB only,

A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-box (STB) able to cope with selective encryption only,

A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB and with selective encryption, A conditional access module in the 2.sup.nd Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB only,

A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-box (STB) able to cope with selective encryption only,

A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-box (STB) able to cope with DVB and with selective encryption, A Smart Card (SC) in a Smart Card Reader (SCR).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any

evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. **Claims 4-6, 9-10, 14, 16, 18, 23, and 36-37 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Candelore, as applied to claims 1 and 2 above, and further in view of Maillard et al. (hereinafter "Maillard"), U.S. Patent No. US 6,714,650, filed on February 12, 1999.

- **Regarding claim 4**, Candelore discloses the system of claim 3.

Candelore does not explicitly disclose the event decryption key is provided on a one-event smart card.

However, in an analogous art Maillard discloses a method for transmitting and recording digital data wherein the event decryption key is provided on a one-event smart card *(col. 5, lines 54-60; col. 6, lines 4-23; the exploitation key is stored on a smart card)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the event decryption key is provided on a one-event smart card to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 5**, Candelore discloses the system of claim 3.

Candelore does not explicitly disclose the event decryption key is provided on a one-limited-period smart card.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the event decryption key is provided on a one-limited-period smart card *(col. 3, lines 22-25; col. 6, lines 4-23; the exploitation key is stored on a smart card)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the event decryption key is provided on a one-limited-period smart card to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 6**, Candelore discloses the system of claim 3.

Candelore does not explicitly disclose the event decryption key in a DVB environment is transmitted in specific EMMs protected by a user encryption key, the corresponding user decryption key being provided in the CAS, on a user smart card or on a user SIM.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the event decryption key in a DVB environment is transmitted in specific EMMs protected by a user encryption key *(col. 2, lines 53-65; the first key is encrypted by a second key)*, the corresponding user decryption key being

provided in the CAS, on a user smart card or on a user SIM *(col. 2, lines 19-24; col. 6, lines 4-12; key stored on a smart card is used to decrypt the encrypted ECM and control word).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the event decryption key in a DVB environment is transmitted in specific EMMs protected by a user encryption key, the corresponding user decryption key being provided in the CAS, on a user smart card or on a user SIM to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67).*

- **Regarding claim 9**, Candelore discloses the system of claim 3.

Candelore does not explicitly disclose conditional access system includes a chip card with decryption circuitry thereon.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein conditional access system includes a chip card with decryption circuitry thereon *(col. 7, lines 44-52; single chip contains descrambling circuitry).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein conditional access system includes a chip card with decryption circuitry

thereon to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 10**, Candelore discloses the system of claim 9.

  Candelore does not explicitly disclose the chip card is a SIM card.

  However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the chip card is a SIM card *(col. 7, lines 44-52; this chip may be embodied in a SIM card)*.

  Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the chip card is a SIM card to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 14**, Candelore discloses the system of claim 13.

  Candelore does not explicitly disclose the event decryption key is transmitted in a GSM network prior to an event and loaded into a SIM or smart card inserted in a SIM or smart card reader of a mobile phone.

  However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the event decryption key is transmitted in a GSM network

prior to an event and loaded into a SIM or smart card inserted in a SIM or smart card reader of a mobile phone *(col. 6, lines 4-10 and 32-43)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the event decryption key is transmitted in a GSM network prior to an event and loaded into a SIM or smart card inserted in a SIM or smart card reader of a mobile phone to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 16**, Candelore discloses the system of claim 3.

Candelore further discloses a head-end encoder for producing the selectively encrypted data stream the head-end encoder including a Common Interface CI *(Figs. 2-3; cable system head-end 122 and 222 are connected with cable system 32 and set-top boxes 36 and 136)*.

Candelore does not explicitly disclose the Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon *(col. 2:3, lines 66-67:1-4; col. 7, lines 44-52)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 18**, Candelore discloses the system of claim 3.

Candelore further discloses a head-end encoder for producing the selectively encrypted data stream, the head-end encoder including a Personal Computer PC *(Figs. 2-3; cable system head-end 122 and 222 are known as PCs)*.

Candelore does not explicitly disclose the Personal Computer PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the Personal Computer PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC *(col. 2, lines 19-24; col. 6, lines 4-12; key stored on a smart card is used to decrypt the encrypted ECM and control word; see also col. 6, lines 31-43)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of

Candelore wherein the Personal Computer PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 23,** Candelore discloses the system of claim 19.

Candelore further discloses the encoder CI module further comprises a high speed interface to a PC, a base transport stream being sent to the PC via the high speed interface to be selectively encrypted by the PC or by a PC peripheral *(pars. 0042-0043, and 0047; Figs. 4 and 7; encrypted audio is transmitted as digitized packets over the A/V channel to set-top boxes)*.

Candelore does not explicitly disclose said PC peripheral being one of the following: a smart card reader SCR for a smart card SC having encryption circuitry thereon; an encryption PCMCIA module having encryption circuitry and forming a SCR for a head-end smart card.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein said PC peripheral being one of the following: a smart card reader SCR for a smart card SC having encryption circuitry thereon *(col. 2:3, lines 66-67:1-4; col. 7, lines 44-52)*; an encryption PCMCIA module having encryption circuitry and forming a SCR for a head-end smart card.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein said PC peripheral being one of the following: a smart card reader SCR for a smart card SC having encryption circuitry thereon; an encryption PCMCIA module having encryption circuitry and forming a SCR for a head-end smart card to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 36**, Candelore discloses a method of producing a scrambled transport stream from a clear transport stream containing digitized multimedia data in successive data packets *(pars. 0010, 0046, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, wherein selected data packets are determined within the clear transport stream *(pars. 0064 and 0089; Figs. 4 and 7; packets are selected for encryption at 250 and 350)*; and the selected data packets are encrypted with an event encryption key *(pars. 0064 and 0089; Figs. 4 and 7; selected packets are passed for encryption to packet encryption process A at step 258 and packet encryption process B at step 262)*.

Candelore does not explicitly disclose the selected data packets are processed to obtain control words CW therefrom; and data packets following each selected data packet are DVB scrambled using control words CW obtained from the preceding selected data packet.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the selected data packets are processed to obtain control words CW therefrom *(col. 1, lines 13-24; col. 6, lines 5-11)*; and data packets following each selected data packet are DVB scrambled using control words CW obtained from the preceding selected data packet *(col. 2, lines 1-11; col. 6, lines 5-11)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the selected data packets are processed to obtain control words CW therefrom; and data packets following each selected data packet are DVB scrambled using control words CW obtained from the preceding selected data packet to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 37**, Candelore and Maillard disclose the method of claim 36.

Candelore further discloses the encrypted selected data packets are inserted in the scrambled transport stream at positions ahead in time with respect to the original positions of the selected data packets in the clear transport stream *(pars. 0054-0055, 0064-0068, and 0089; Figs. 3-4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; packet is encrypted as a part of the encryption time slice; the EA and EB packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same)*.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. US 5,805,700 to Nardone et al.
U.S. Patent No. US 7,106,749 to Darshan et al.
U.S. Patent No. US 6,415,031 to Colligan et al.
U.S. Patent Application No. US 2002/0194613 by Unger.
U.S. Patent Application No. US 2002/0146118 by DiSanto et al.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137